Our Ref.: **36-1287**
A25470 USw

U.S. PATENT APPLICATION

Inventor(s): Robert D. Spindley
Nigel C.V. Smith

Invention: COMMUNICATIONS NETWORK

NIXON & VANDERHYE P.C.
ATTORNEYS AT LAW
1100 NORTH GLEBE ROAD
8TH FLOOR
ARLINGTON, VIRGINIA 22201-4714
(703) 816-4000
Facsimile (703) 816-4100

SPECIFICATION

10PRTS

09/171960

300 Rec'd PCT/PTO 29 OCT 1998

Communications Network

SUB B1

The present invention relates to a communications network, and in particular to the handling of control signals passing between a network node and a source external to the network.

B

2. Related Art

In the past, large communications networks, such as public switched telephony networks (PSTNs), have been used under the sole control of a single operator, and interactions with other networks and with devices external to the network have been simple and restricted in nature. Such networks have therefore been designed to offer a wide range of control functions within the network infrastructure but without these functions being exposed outside of the network. In recent years however, there has been an increasing need to interface networks with other networks, and to make at least part of the network functionality available to third parties who wish to provide a service to customers connected to the network. This then raises the problem of unauthorised use of the network. For example, the network operator may allow a third party to connect to an access node for processing of calls which originate or terminate in the network. This access must not be exploited by the third party for transfer routing of calls to or from customers located outside of the network without prior agreement. To prevent such unauthorised use, it has been necessary hitherto to screen all such traffic in order to bar any illicit use of the access point. However, this imposes heavy burdens in terms of data management, data storage and processing, and becomes increasingly impractical as the number of parties accessing the network in this way increases. To avoid such processing overheads, whilst preventing unauthorised access to the network, it has been proposed to use a different signalling protocol with restricted capabilities on the access link to that used within the network. This however necessitates modification of the access node in order to handle the additional protocol, and involves additional costs for both the network operator and the party accessing the network.

B

BRIEF SUMMARY OF THE INVENTION

According to a first aspect of the present invention, there is provided a method of operating a node in a communications network, which node is in use connected to a signal source external to the communications network, the method comprising:

a) receiving from the said signal source signals which include a control field, which control field takes one of a plurality of possible values, and the subsequent handling of the said signal by the network being controlled according to the value of the control field;

b) overwriting the control field with a value from a restricted subset of the plurality of possible values; and

c) subsequently processing the signal in the network in dependence upon the said value overwritten in step (b).

According to a second aspect of the present invention, there is provided a method of operating a node in a communications network, which node is in use connected to a signal source external to the communications network, the method comprising:

a) receiving from the said signal source signals which include a control field, which control field takes one of a plurality of possible values, and the subsequent handling of the said signal by the network being controlled according to the value of the control field;

b) within a lower level of a messaging protocol running on the node, and prior to the processing of the signal by higher level functions running on the node, overwriting the control field with a value from a restricted subset of the plurality of possible values; and

c) subsequently processing the signal in the network in dependence upon the said value overwritten in step (b).

The present invention provides effective control of the use made of access to the network by an external party, without requiring continual high-level screening of traffic through the node, and without it being necessary to use a different signalling protocol to that adopted elsewhere in the network. This is achieved by overwriting control fields in the incoming signalling with allowed values determined by the network operator. The subsequent handling of the signal, and any consequent processing by the network, for example of a voice call, is then constrained by the values written in the control fields. It is particularly advantageous to overwrite the control field within a low level of the messaging protocol used to communicate with the node. In particular this may be done within the signalling link layer, that is the data link layer, layer 2 of the ISO 7-layer model. It is found that by providing security at this low level, the solution offered by the

present invention is made fast, robust and readily scaleable, by contrast with prior art systems which operate at an application level.

Preferably the said control field is a routing control field, and the overwriting of the routing control field with a predetermined value in step (b) limits the routing of signals to or from the external source to part only of the communications network. Preferably the routing of signals to or from the external source is limited to a point-to-point connection between the external source and the node.

Often, a third party will be given a connection to an access node with the intention that it should be used as a simple point-to-point link for direct transfer of signals into or out of the network. However, depending on the values set in the routing control fields of the incoming signals, the third party might extend its access to further nodes beyond the original access node. This might be done, for example, in order to implement transfer routing through the network to another party outside of the network. This preferred aspect of the invention prevents this by overwriting the routing control fields. In the case of a network employing ITU-T Signalling System No. 7 (SS7), the relevant control fields are the originating point code (OPC) and destination point code (DPC) and the access node overwrites one or both of these codes. The OPC may be overwritten with the point code of the external signal source, and the DPC may be overwritten with the point code of the access node.

SS7 is a widely adopted and stable protocol for common channel signalling in communications networks. It is a highly flexible protocol which makes possible a wide range of control functions. The present invention is particularly advantageous in this context since it allows use of the SS7 protocol without modification for access signalling whilst effectively constraining the use made of the protocol.

The invention is by no means limited to use with routing control codes. It may also advantageously be implemented, for example, by overwriting a code which identifies the originating network for a signal. This code may be the Network Identifier Code specified in the SS7 NUP (national user part) protocol, and published in the BT National Requirements document BTNR 167, Issue 3, July 1987, Vol. 1. Overwriting this code can provide another means to prevent use of the network as a transit network, or can be used to ensure appropriate billing of

traffic when this depends on the originating network. Overwriting such a code may be carried out in addition to, or alternatively in place of, overwriting point codes.

The invention is not limited to use with SS7, but may also be used with different network protocols, including, for example, Internet Protocol or the X25 packet data protocol.

According to a second aspect of the present invention, there is provided a method of operating a communications network comprising:

a) communicating control signals between nodes of the network, which control signals conform to a predetermined signalling protocol;

b) at one of the said nodes, receiving from a signal source external to the network signals conforming to the said predetermined protocol and including a control field, which control field takes one of a plurality of possible values;

c) overwriting the control field with a value from a restricted subset of the plurality of possible values; and

d) subsequently processing the signal in the network in dependence upon the said value overwritten in step (c).

According to a further aspect of the present invention there is provided node suitable for connection in a communications network and comprising:

a) a network interface for connection to the communications network;

b) a signal interface for connection to a signal source external to the communications network;

c) means for overwriting with one of a subset of predetermined values a control field in a signal received via the signal interface from the signal source; and

d) signal processing means for processing the said signal in dependence upon the value of the said control field.

According to a further aspect of the present invention, there is provided a node suitable for connection in a communications network and comprising:

a) a network interface for connection to the communications network;

b) a signal interface for connection to a signal source external to the communications network;

c) means connected to the signal interface for overwriting, within a lower level of a messaging protocol, a control field in a signal received via the signal interface from the signal source with one of a subset of predetermined values; and

d) signal processing means for processing the said signal in dependence upon the value of the said control field.

The invention also encompasses networks adapted to operate in accordance with the first or second aspects.

BRIEF DESCRIPTION OF THE DRAWINGS

Systems embodying the present invention will now be described in further detail, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a schematic of a network embodying the invention;

Figure 2 is a schematic showing switching points in the network of Figure 1;

Figure 3 is a diagram showing a SS7 protocol stack;

Figure 4 is a diagram showing the format of a SS7 Message Signalling Unit (MSU);

Figure 5 is an SDL (Specification and Description Language) definition of processes implementing the present invention;

Figure 6 is an SDL definition of an alternative embodiment;

Figure 7 is a further SDL diagram, indicating the operation point of the invention;

Figure 8 is a diagram showing an example digital local exchange;

Figure 9 is a diagram showing in further detail the signalling hardware module in the exchange of Figure 8; and

Figure 10 shows a further embodiment of the invention in a network using internet protocols.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

A telecommunications network which uses an IN (Intelligent Network) architecture includes a service control point (SCP) 1. The service control point 1 is connected to digital trunk switching units 2 ,3 (also termed "trunk switches") and to digital local exchanges (DLE's) 4,5 (also termed "local switches"). The switches in this example also function as service switching points (SSP's). At certain points during the progress of a call, the SSP's transfer information related to the call to the service control point. The service control point carries out functions such as number translation, and may control collection of additional call related

information. The trunk switches communicate with each other and with the service control point via the signalling network 6. The components so far described are all within the network, in the region referenced a, and are under the control of the network operator. A third party node (3ptyN) is located outside of the network in the region referenced b and connects to the network at an access node using the signalling protocol of the common channel signalling network. In the present example, this protocol is ITU-T Signalling System No. 7 (SS7). For a full description of SS7, reference is made to the ITU recommendations {Q.700/1/2/3/4/5/6/7/8}. - Specification of signalling system No.7; and the journal British Telecommunications Engineering, vol. 7 , part 1, April 1988, "CCITT Signalling System No.7".

Figure 2 shows schematically SS7 switching points referenced A, B and C. These correspond respectively to trunk switch 3, to the third party node and to the SCP 1. The operator of the network in region A sanctions access by the third party to the network, for example in order to provide a number translation service to customers connected to the network. It is agreed with the service provider, or other operator that the third party node will use a direct SS7 signalling link to trunk switch 3, and will not access other nodes of the network such as the SCP 1, and will not use access to the SS7 signalling network for transfer routing of calls.

Figure 3 shows the SS7 protocol stack. One characteristic feature of the SS7 protocol is the use of modular structure in which application-dependent functions in a layer termed the *User part* 32 are supported by a lower level transport protocol, termed the *Message transfer part* (MTP) 31 . The MTP has a three-level structure. Level 1 includes the physical signalling data link. In a digital network this is provided by a predetermined one of a number of time slots in a PCM system operating at, e.g. 64kbit/s. Level 2 includes the hardware of the signalling terminal together with the functions necessary to translate between processor software signals and the bit stream of the signalling data link. Level 3 comprises signalling network functions including functions for the transfer of messages, for the reconfiguration of routes after failure, and for sending information about faults in the signalling network.

Figure 4 shows the format of a message signalling unit (MSU) which is handled by a Signal Message Handling function of Level 3 of MTP. A message is delivered to the Level 3 of the MTP which adds some information and then passes

it to Level 2. Level 2 headers are added and the MSU is output for transmission on the SS7 signalling network. In addition to the Level 2 headers, and user information for use by the Level 4 application, the MSU contains the following fields:

DPC - destination point code

OPC - originating point code

SIO - service information octet

SLS - signalling link selection.

The OPC and DPC fields are each 14 bits long, and in conjunction with the Network Indicator code contained in the SIO field, form the complete point code of a particular node.

In the present example, an interconnect agreement between the network operator specifies that SS7 traffic between nodes B and A should be limited to a simple duplex connection. If this agreement is adhered to, then all SS7 MSU's sent by the node B to the access node A should have code-A in the DPC field, where code-A is the 14 bit point code of the access node A. Similarly the MSU's should have code-B in the OPC field, where code-B is the 14 bit point code of the interconnected network or service provider, at node B. If however the data is incorrectly defined at the nodes, then these fields may contain other values. For example, in implementing transfer routing, the service node might write a value for the DPC field which is not code-A, but is the point code of another node, outside of region a of the network. To eliminate the possibility of such breaches, without imposing a heavy processing overhead, the signalling link hardware in the access node, which implements Level 2 of the MTP, overwrites the OPC and DPC fields of SS7 signalling from the third party node with the allowed values, namely code-B and code-A respectively, also ensuring that the correct Network Indicator is applied. In addition, or alternatively, other parts of the MSU may be overwritten. In particular, as discussed in the introduction above, the NUP (national user part) identifier may be overwritten with the value corresponding to the party operating node B.

Figure 5 is an SDL diagram showing the modifications made to Level 2 MTP in order to implement the policing function described above. Feature data for each signalling link indicates whether the relevant link is to be policed or not. In step s1 the feature data is tested. If the link is to be policed then in step s2 the

OPC of the incoming MSU is tested to see whether it has the allowed value. If it has not, then in step s3 the OPC is overwritten with the allowed value and in step s4 the policing violation is notified to an alarm process. Similarly, in step s5, the DPC is tested to see whether it has the allowed value, and in steps s6 and s7 it is overwritten and a policing violation notified if the DPC is not the allowed value for that link. Following these steps, the Level 2 processing of signalling continues in a conventional fashion, and the resulting MSU's are passed to Level 3 of the MTP, where routing and message handling functions are carried out on the basis of the DPC and OPC values which are guaranteed to be permitted value. Accordingly further policing is not required in Level 3. The process of Figure 5 is shown by way of example only, and other implementations are possible. For example, the DPC may be checked, and if necessary may be overwritten, prior to the OPC being checked.

Figure 6 shows the modified SDL of an alternative embodiment. Initially, as in the first embodiment, the feature data is tested to determine whether the policing flag has been set (s61). In addition, a test is carried out to determine whether another flag in the feature data indicating that an alarm function is required has been set (s62). If this flag has not been set, that is to say if policing is required without an alarm function, then in steps s63 and s64 the OPC and DPC codes are overwritten unconditionally. Otherwise, in steps s65 and s66, the OPC and DPC codes are tested, and the codes overwritten and alarms raised depending on the outcome of the tests, as described previously in relation to the first embodiment.

The modified SDL of the first or second embodiments may be substituted in the Basic Transmission Control SDL of the SS7 standard published in ITU Q.703 Figure 14, sheet 5 of 6. The position of the new SDL required by the invention is illustrated in Figure 7, in which the new SDL is shown in bold. In implementing the invention, an instance of the processes defined by the SDL is created for each link handled by the node. In this way, the policing function is inherently scaleable, by contrast with methods previously adopted in which policing was carried out entirely in software and in a much higher level of the protocol stack, where one function would be required to handle many links.

Figure 8 shows an example of a network node, in this case a digital local exchange, implementing the invention. It will be understood that this is chosen by

way of illustration only, and that the invention may be implemented on a wide range of different platforms. The principal elements of the exchange comprise transmission equipment 81, a digital switch 82, signalling transport hardware for the signalling links 83, signalling hardware modules 84, and processor systems 85 that control all the elements for either normal call processing or management activity. Each signalling transport hardware modules terminates a number, e.g. 16, signal links, each link comprising a pair of incoming and outgoing signals respectively. For each link there is provided within the SS7 signalling transport hardware, a respective input buffer and output buffer, and cyclic redundancy check (CRC) system that performs basic error checking on the received message. If the computed check-sum value has the expected value, then the signal is passed upwards to the signalling processor and subsequently on to the call processing system which executes basic call processing functions. If however, a bit error is encountered the message is immediately discarded. The processor system constantly monitors the buffers to ensure that when an incoming signal is received the input buffers can accommodate it. If full, the processor writes a TFC (transfer controlled) message via the output buffer of the respective link. Otherwise the signal is transferred to the other signalling hardware 84. The other signalling hardware discriminates signals addressed to the node from other signals using the MTP OPC DPC codes. If the DPC is not that of this node, then it directs the signal back through the signalling transport hardware to a relevant output link. In addition, in a node embodying the invention, the other signalling hardware carries out a policing function which overwrites OPC and DPC codes, using the processes defined in the SDL described above. Figure 9 shows in further detail the structure of the other signalling hardware. A microprocessor 91 is linked by a control interface 92 to firmware 93, which may include an EPROM, and to buffers B1, B2,... . Although for ease of illustration only two buffers are shown, in practice buffer capacity is provided for each link handled by the signalling hardware. The policing function already described is executed by software processes running on the microprocessor 91, in combination with firmware and hardware operations. In particular, instructions to overwrite selected bytes held in a buffer are downloaded from the microprocessor to the firmware. In this example, this results in the byte position corresponding to the NUP Network Identifier, the byte position corresponding to the OPC and the byte position

corresponding to the DPC being overwritten with predetermined allowed values which are specific to a particular SS7 signalling link, referenced Link 1. Then the signal is passed upwards to the call processing system which executes basic call processing functions. The signalling hardware functions autonomously, but may pass alarm signals, such as those generated as a result of checking OPC/DPC values, to the management systems.

Although in Figure 8 just a single instance of each element is shown, in practice the exchange will usually comprise a single Call Processing System connected to multiple processes. Each processor may consolidate traffic from a hierarchy of transport processes and signalling hardware modules.

Figure 10 shows a future alternative embodiment of the invention. In this case region a is private network using internet protocols, i.e. an intranet. A node 102 external to the private network, in region b, is connected to a node 101 in region a. This might be done, for example, in order to provide access to certain web pages running on a web server at the node in region a. The node in region has, in this example, internet address 111.111.1.111 and the node in region b has internet address 123.123.1.123. In order to prevent access by the region b node to other nodes 103, 104, node 101 overwrites the destination internet address and the return internet address of incoming packets from node 102 with the allowed values, namely 111.111.1.111 and 123.123.1.123. As in the previous examples, an alarm may be raised if either of these addresses in an incoming packet has an illicit value. The steps of testing and overwriting the network addresses is carried out in the network interface, for example in an X25 or ethernet interface card, before the packet is passed to the internet protocol (IP) layer of the software on the node 101. The function of the IP layer can therefore remain entirely conventional and it is not necessary at this level to distinguish between packets originating elsewhere on the intranet and packets originating from an external source such as node 102.